

1 PROTECTING IMAGES WITH AN IMAGE WATERMARK

2 FIELD OF THE INVENTION

3 This application relates to the field of digital imaging. It is
4 more specifically concerned with the insertion and detection of
5 an identifying mark on a work-piece.

6 BACKGROUND OF THE INVENTION

7 It is a constant endeavor to find improved techniques of placing
8 a visible or invisible identifying mark on an image. This is
9 generally useful to establish ownership, origin and authenticity,
10 and also to discourage those who might wish to purloin or
11 misappropriate the work. Identifying marks are also useful to
12 give evidence of unauthorized alteration or disclosure.

13 Visible marks are herein classified as being either visible
14 robust or visible fragile. A mark is classified as *visible robust*
15 if it can be seen by the unaided eye and cannot be easily removed
16 from the work-piece, if at all, without leaving telltale
17 evidence. It is classified as *visible fragile* if the mark itself
18 is visibly altered by an attempt to alter the work-piece or its
19 wrapper.

20 Invisible marks are herein classified relative to the appearance
21 of that mark to a human being with normal visual acuity. A mark
22 on an image is classified as having an invisibility

1 classification level of *undetectably invisible* if, when the image
2 without the marking is displayed together with an image copy with
3 the marking, the human being is equally likely to select either
4 of these copies. An undetectably invisible mark is below or at
5 the human being's just noticeable difference. A mark on an image
6 is classified as having an invisibility classification level of
7 *subliminally invisible* if the mark is not distracting to the
8 human viewer, although it is above the human being's just
9 noticeable difference. An image mark is classified as being
10 *marginally invisible* if it does not cause the marked image to
11 lose its usefulness or value because of the mark. An image
12 marking is classified as being *poorly invisible* if the marking
13 causes a reduction in the usefulness and/or value of the image.

14 Presently, both visible and invisible markings of hardcopy
15 documents are used as a generally dependable method of
16 establishing ownership and authenticity. These time-tested
17 methods are also useful for marking a "softcopy" *digitized image*,
18 also referred to herein as an image. A digitized image is an
19 abstraction of a physical image that has been scanned and stored
20 in a computer's memory as rectangular arrays of numbers
21 corresponding to that image's (one or more) color planes. Each
22 array element corresponding to a very small area of the physical
23 image is called a picture element, or *pixel*. The numeric value
24 associated with each pixel for a monochrome image represents the
25 magnitude of its average brightness on its single color (black
26 and white) plane. For a color image, each pixel has values
27 associated and representing the magnitude or average brightness
28 of its *tristimulus* color components representing its three color
29 planes. Other image representations have more than three color

1 components for each pixel. A different component value is
2 associated with each different one of the image's color planes.

3 In what follows, whenever reference is made to color planes it is
4 understood to include any number of color planes used by a
5 particular image's digitizing technique to define the pixel's
6 color characteristics. This includes the case when there is only
7 a single plane defining a monochrome image.

8 A digitized image is recognizable as an image to a human viewer
9 only when the individual pixels are displayed as dots of white or
10 colored light on a display or as dots of black or colored inks or
11 dyes on a hardcopy. Pixels are normally spaced so closely as to
12 be unresolvable by the human visual system. This results in the
13 fusion of neighboring pixels by the human visual system into a
14 representation of the original physical image. Image fusion by
15 the human visual system makes invisible marking, or relatively
16 invisible marking, of images possible. This property is fully
17 exploited by the methods described here to both impart upon a
18 digitized image an invisible watermark to a desired invisibility
19 classification, and to subsequently demonstrate its existence.
20 The imparting and demonstrated detection of a robust invisible
21 marking on digitized images, herein called invisible
22 watermarking, are a primary aspect of the present invention.

23 ***PROPERTIES OF A ROBUST INVISIBLE WATERMARK***

24 A proper invisible watermarking technique that imparts an
25 invisible watermark upon a proprietary digitized image should
26 satisfy several properties. The imparted watermark should appear

1 to be invisible to any person having normal or corrected visual
2 accommodation to a desired invisibility classification level.
3 Clearly, the degree of marking is a dichotomy. A balance has to
4 be struck between protecting the image from unauthorized uses and
5 not having the watermark unpleasantly alter the appearance of the
6 image. This generally means that a recognizable pattern should
7 not appear in the marked image when the watermark is applied to a
8 uniform color plane. This requirement discourages marking the
9 image by varying the hue of its pixels, since the human visual
10 system is significantly more sensitive to alterations in hue than
11 in brightness. The requirement can be satisfied by a technique
12 based on varying pixel brightness implemented in a proper way. A
13 technique based on varying pixel brightness also allows the same
14 marking technique applied to color images to be equally
15 applicable to monochrome images.

16 Another property of a proper invisible watermarking technique is
17 that it should have a detection scheme such that the probability
18 of a false-positive detection is vanishingly small. For purposes
19 of the present invention, the probability of detection of a
20 watermark in an image when one does not exist should be less than
21 one in a million. There is generally little difficulty satisfying
22 this requirement when the technique is statistically based.

23 Still another property of a proper watermarking technique is that
24 it should be possible to vary the degree of marking applied to an
25 image. In this way, the watermark can be made as detectable as
26 necessary by the particular application. This property is
27 important in highly textured images where it is often necessary
28 to increase the intensity of the mark to increase its likelihood
29 of detection. This is in contradistinction with images that have

1 low contrast in which it is advantageous to reduce the marking
2 intensity to lessen undesirable visible artifacts of the
3 watermark itself.

4 It is also highly desirable that when detected the demonstrated
5 existence of the watermark should be translatable to a
6 recognizable visual image having relatively bold features with a
7 high contrast ratio. Features of a demonstrated visual image that
8 are not relatively bold may otherwise be difficult to show if the
9 watermark has been attacked in attempts to defeat its protection.

10 Finally, the imparted watermark should be robust in that it
11 should be very difficult to be removed or rendered undetectable.
12 It should survive such image manipulations that in themselves do
13 not damage the image beyond usability. This includes, but is not
14 limited to, JPEG "lossy" compression, image rotation, linear or
15 nonlinear resizing, brightening, sharpening, "despeckling," pixel
16 editing, and the superposition of a correlated or uncorrelated
17 noise field upon the image. Attempts to defeat or remove the
18 watermark should be generally more laborious and costly than
19 purchasing rights to use the image. If the image is of rare
20 value, it is desirable that the watermark be so difficult to
21 remove that telltale traces of it can almost always be recovered.

22 SUMMARY OF THE INVENTION

23 An aspect of the present invention is to provide a method for
24 imparting a watermark onto a digitized image comprising the steps
25 of providing the digitized image, and multiplying the brightness
26 data associated with at least one of the image pixels by a
27 predetermined brightness multiplying factor. The image includes a

1 plurality of pixels, wherein each of the pixels includes
2 brightness data that represents one brightness value if the image
3 is monochrome, or a plurality of brightness data values if the
4 image has multiple colors. A brightness data value of a pixel and
5 a color component or component are hereinafter used to mean the
6 same thing, and are therefore to be considered interchangeable.
7 In an embodiment, the brightness multiplying factor ranges from
8 0.5 to 1.0. Other smaller or larger factors are useful in some
9 image applications dependent upon particular desired watermarking
10 results. The brightness multiplying factor has a relationship
11 with a number taken from a random number sequence and the
12 relationship is a linear remapping to provide a desired
13 modulation strength.

14 In an embodiment, each of the pixels has a row and a column
15 location in an array representing the digitized image, and the
16 brightness multiplying factor employs a different sequential
17 combination of numbers from a robust random number sequence in
18 sequential correspondence to the row and column location.

19 Another aspect of the present invention is to provide a method
20 for generating a watermarked image wherein a watermark is
21 imparted onto a digitized image having a plurality of original
22 pixels, each pixel having original brightness values. The method
23 includes the step of providing a digitized watermarking plane
24 comprising a plurality of watermarking elements, each having a
25 brightness multiplying factor and having one-to-one positional
26 correspondence with the original pixels. It also includes the
27 step of producing a watermarked image by multiplying the original
28 brightness values of each of the original pixels by the
29 brightness multiplying factor of a corresponding one of the

1 watermarking elements wherein the watermark is invisible. In an
2 embodiment, when the original image forms an original plane and
3 the watermarking plane is smaller than the original plane, the
4 method further includes the step of extending the watermarking
5 plane by tiling such that the watermarking plane covers the
6 original plane and/or further comprises the step of truncating
7 the watermarking plane such that the watermarking plane covers
8 the original plane, upon determining that the watermarking plane
9 extends beyond the original plane.

10 Another aspect of the present invention is to provide a method
11 for forming a watermarking plane including a plurality of
12 elements each having a multiplying value. The method comprises
13 the steps of: generating a robust random sequence of integers
14 having a first plurality of bits; linearly remapping the random
15 sequence to form a remapped sequence of brightness multiplying
16 factors to provide a desired modulation strength; computing a
17 discrete Fourier transform of the remapped sequence to form a
18 Fourier sequence having frequency coordinates; expanding the
19 frequency coordinates to form an expanded sequence; and computing
20 an inverse Fourier transform of the expanded sequence to obtain a
21 watermarking sequence of values.

22 An embodiment further includes one or more of the following: the
23 step of expanding is accomplished by zero-padding; the method
24 further comprises a step of employing the watermarking sequence
25 to provide the multiplying value for each of the elements; the
26 method further comprises the steps of hard clipping the
27 watermarking sequence to form a hard-clipped sequence having
28 sequence members, and utilizing a different one of the sequence
29 members to provide the multiplying value for each of the

1 elements; the method further comprises the steps of adjusting the
2 watermarking sequence to form a normalized sequence of values
3 having a mean and a median equal to the difference between unity
4 and the modulation strength, and having a maximum of unity, and
5 employing the normalized sequence to provide the multiplying
6 value for each of the elements; the method further comprises the
7 steps of providing an unmarked original image having a plurality
8 of original pixels, each of the pixels having at least one
9 component, wherein a first number of the original pixels is
10 greater than a second number of the plurality of elements,
11 expanding the watermarking plane by tiling to cover the unmarked
12 original image such that one of each of the pixels has one
13 corresponding element from the elements; and multiplying the at
14 least one component of each of the pixels by the multiplying
15 value of the corresponding element.

16 Still another aspect of the present invention is to provide a
17 method for detecting a watermark in a marked image. The marked
18 image is marked by a watermarking plane which has a plurality of
19 watermarking elements. Each of the image pixels has at least one
20 component and each of the watermarking elements has a brightness
21 multiplying factor. The method employs a selector having at least
22 one element and a visualizer having at least one pixel and at
23 least one counter, said at least one counter to store the
24 comparison data resulting from comparisons for each of a
25 plurality of selector elements and positions; said comparison
26 data resulting from the comparison of the statistical brightness
27 of each image color component, relative to its neighboring color
28 components in the same plane, with the statistical magnitude of
29 each corresponding brightness multiplying factor, relative to its
30 neighboring multiplying factors. The method further comprises the

1 step of displaying a visualizer-coincidence image such that a
2 user can make a determination as to whether the pattern encoded
3 by the visualizer pixels is recognizable and thereby, whether the
4 watermark is detected.

5 Further, it is an aspect of the present invention to provide an
6 alternative method and apparatus for imparting a watermark into
7 a digitized image that includes the step of providing the
8 digitized image and the step of adding at least one predetermined
9 brightness adjusting value to the brightness data associated with
10 at least one of the image pixels. The image includes a plurality
11 of pixels, wherein each of the pixels includes brightness data
12 that represents one component if the image is monochrome, or a
13 plurality of components if the image has multiple colors. The
14 step of "adding a predetermined brightness data value to a
15 component" is used in the same way as the step of "multiplying a
16 component by a predetermined brightness multiplying factor",
17 where the component is associated with at least one of the image
18 pixels. Under conditions that will be specified, the step of
19 adding achieves image watermarking results which are similar in
20 every manner and respect to the step of multiplying. The additive
21 brightness adjusting values may be positive or negative, and a
22 color component altered by the step of adding increase or
23 decrease accordingly.

24 In another aspect of a general embodiment, the components of all
25 image pixels, or all image pixels in a specified image portion,
26 are each modified by an associated brightness adjusting factor.

27 In another particular embodiment, each of the pixels has a row
28 and a column location in an array representing the digitized

1 image, and the brightness adjusting factors for each pixel employ
2 a different sequential combination of numbers from a different
3 robust random number sequence in sequential correspondence to the
4 row and column location.

5 Another aspect of the present invention is to provide a method
6 for generating a watermarked image wherein watermarks are
7 imparted into a digitized image by having a plurality of original
8 watermarking elements, with each of the elements having an
9 original brightness adjusting value.

10 Another aspect of the present invention is to provide a method
11 for forming watermarking planes. Each watermarking plane includes
12 a plurality of elements with at least one brightness adjusting
13 value derived from each element.

14 Still another aspect of the present invention is to provide a
15 method for improving the probability of detection of a watermark
16 in a marked image or a derived copy of a marked image. The marked
17 image is marked by a watermarking plane which has a plurality of
18 watermarking elements. The method applies a two-dimensional
19 **blurring filter** to the marked image or derived copy of a marked
20 image prior to attempted detection of the imparted watermark.

21 BRIEF DESCRIPTION OF THE DRAWINGS

22 These and other objects, features, and advantages of the present
23 invention will become apparent upon further consideration of the
24 following detailed description of the invention when read in
25 conjunction with the drawing figures, in which:

1 FIG. 1 shows a block diagram of an image capture and distribution
2 system suitable for use in accordance with an embodiment of the
3 present invention.

4 FIG. 2 shows an embodiment for forming a watermarking plane in
5 accordance with the present invention.

6 FIG. 3 shows an embodiment for the steps of watermark imparting.

7 FIG. 4 shows an overview of the steps for image alignment.

8
9
10 FIG. 5 shows the steps for a coarse alignment of a marked image
11 with a correlation reference plane.

12 FIG. 6 shows the steps for a fine alignment of a marked image
13 with a correlation reference plane.

14 FIG. 7 shows the steps for finding a watermark in a marked image.

15 FIG. 8 shows a random positioning of the selector array over the
16 watermarking plane and the image planes.

17 FIG. 9 shows a typical visualizer pattern.

18
19 FIG. 10 shows a method of verification of the presence of the
20 watermark.

FIG. 11 shows a detection resulting from the visualizer of Figure
9 for a watermarking made at a modulation strength of 1%.

1 FIG. 12 shows a detection resulting from the visualizer of Figure
2 9 for a watermarking made at a modulation strength of 2%.

3 FIG. 13 shows a detection resulting from the visualizer of Figure
4 9 for a watermarking made at a modulation strength of 4%.

5 FIG. 14 shows a detection resulting when the image has no
6 watermark.

7 FIG. 15 shows the steps for an alternate method of finding a
8 watermark in a marked image.

9 FIG. 16 shows an enlarged segment of a watermarked image, having
10 been watermarked at a modulation strength of 2.5%, that is used
11 as the reference image.

12 FIG. 17 shows the enlarged segment of the reference image after
13 it has been prepared for printing by screening, has been printed
14 and has been scanned to form the derivative image.

15 FIG. 18 shows the enlarged segment of the derivative image that
16 has been acted upon by a blurring filter to form the filtered
17 image.

18 FIG. 19 shows a visualizer-coincidence image resulting from a
19 watermark detection made on the reference image.

20 FIG. 20 shows a visualizer-coincidence image resulting from a
21 watermark detection made on the derivative image.

1 FIG. 21 shows a visualizer-coincidence image resulting from a
2 watermark detection made on the filtered image.

3 DETAILED DESCRIPTION OF THE INVENTION

4 The present invention provides a robust means of watermarking a
5 digitized image with a highly random sequence of pixel brightness
6 multipliers. The random sequence is formed from four
7 'robust-watermarking-parameters' selected and known only by the
8 marker and/or the marking entity. A watermarking plane is
9 generated which has an element array with one-to-one element
10 correspondence to the color component array or arrays of the
11 digitized image being marked. Each element of the watermarking
12 plane is assigned a random value dependent upon a robust random
13 sequence and a specified brightness modulation strength. The so
14 generated watermarking plane is imparted onto the digitized image
15 by multiplying the brightness value or values of each pixel by
16 its corresponding element value in the watermarking plane. The
17 resulting modified brightness values impart the random and
18 relatively invisible watermark onto the digitized image.
19 Detection of an imparted watermark requires knowing the
20 watermarking plane with which the watermark was imparted.
21 Regeneration of the watermarking plane requires knowledge of the
22 robust-marking-parameters used in its formulation. This is
23 generally only known to the marker and/or marking entity. Once
24 regenerated the watermarking plane is used together with a
25 verifying image located in a 'visualizer' to demonstrate the
26 existence of the watermark.

27 Brightness modulation is the essence of watermark imparting
28 according to the present invention. Pixel brightness, as used

1 herein, expresses the brightness of a visual stimulus in terms of
2 the CIE 1931 Standard Colorimetric Observer and Coordinate System
3 tristimulus component brightness X , Y and Z that correspond to a
4 matching mixture of three reference stimuli. If the image is
5 monochrome, pixel brightness expresses the brightness of a visual
6 stimulus in terms of the CIE 1931 Standard Coordinate System
7 photopic brightness Y , and components X and Z have no meaning. A
8 more detailed description of pixel brightness is found in G.
9 Wyszecki and W. S. Styles, "Color Science: Concepts and Methods,
10 Quantitative Data and Formulae," John Wiley & Sons, Inc. (2nd
11 ed.), New York, 1982, pp. 164-169, incorporated herein by
12 reference in its entirety. The CIE 1931 standard specifies three
13 particular reference stimuli. The stimuli are radiometric
14 quantities, and as such are expressed in radiometric units such
15 as watts. Grassmann's law, on which nearly all of modern
16 colorimetry is based, requires use of the three specific
17 reference stimuli, or three others that are distinct linear
18 combinations of them. This is discussed in D. B. Judd and G.
19 Wyszecki, "Color in Business, Science, and Industry," (3rd ed.),
20 John Wiley & Sons, Inc., New York, 1975, pp. 45-47, incorporated
21 herein by reference in its entirety. By modifying only a pixel's
22 brightness, its color, represented by its hue and saturation, is
23 not changed. This is accomplished by preserving the ratios of $X:Y$
24 and $Z:Y$ while changing the magnitude of Y . A pixel represented in
25 any nonlinear color space, such as the color space of the
26 subtractive dyes Cyan, Magenta, Yellow and Black (CMYK) used in
27 color printing, will be translated to the X,Y,Z color space (or
28 to a color space linearly related to it) before the pixel's
29 brightness is modified.

1 Figure 1 shows a block diagram of a system embodiment for
2 imparting a relatively invisible watermark on a digitized image
3 in accordance with the present invention. Figure 1 shows an image
4 capture and distribution system 150 suitable for use in
5 accordance with an embodiment of the present invention. A scanner
6 100 captures image data 101 from a physical source 102. The
7 physical source 102 is typically a painting or photograph. The
8 image sends data 101 to a digital computer 104. The computer 104
9 includes a working storage 106 that is typically embodied in the
10 computer's random access memory, an image storage system 108 that
11 is often a conventional hard disk drive, and an image archive 110
12 that can be a tape or disk storage. The computer 104 also
13 includes a number of software modules. These include front end
14 image processing software 112 that performs image processing such
15 as scaling and enhancement of the image data provided by the
16 scanner 100. It also includes color preserving watermarking
17 software 114 operating in accordance with the principles of the
18 present invention, and back-end image processing software 116
19 that performs other processing functions such as compression on
20 the watermarked image. Most often, the unprocessed or front-end
21 digitized original image 101 is sent to the image archive 110 for
22 preservation in unwatermarked form.

23 An alternate embodiment has the original image already available
24 in digitized form 101 without requiring a scanner 100. The
25 watermarking software 114 applies a relatively invisible
26 watermark to the digitized image 101 in accordance with the
27 principles of the present invention. The watermarking process can
28 also be performed on a copy of an archived image or on other
29 scanned and processed image data, which has been loaded in whole
30 or in part, into the computer's working storage 106.

1 The processed, watermarked and compressed image produced by the
2 combination of the software modules 112-116 is sent from the
3 working storage 106 or image storage 108 to an image server 118
4 that is connected to a digital network 120. When appropriate, the
5 digital network is interconnected with a Local Area Network
6 (LAN), a Wide Area Network (WAN) such as the Internet, or both.
7 Other systems 122 connected to the digital network 120 can
8 request and receive images stored on the image server 118 via the
9 digital network 120. In some cases, the systems can then display
10 the received images on a display device 124 and/or print the
11 images on a graphics capable printer 126. Those skilled in the
12 art will recognize that there are many other system
13 configurations in which the present invention could be employed.
14 The system of Figure 1 is generally also useful for detecting and
15 demonstrating the existence of the watermark in a manner such as
16 those described subsequently.

17 **MARKING AN IMAGE WITH A ROBUST WATERMARK**

18
19 In one embodiment, the watermark imparted onto the digitized
20 image is a monochrome pattern, herein called "the watermarking
21 plane," that overlays the digitized image. The pattern is
22 embodied by selecting its element values from a robust random
23 sequence formed from a group of robust sequence generating
24 parameters. The parameters are used to generate a generally
25 strongly encrypted random sequence in a manner well known to
26 those skilled in the art. These parameters are herein referred to
27 as the 'robust-watermarking-parameters'. In a preferred
28 embodiment, these parameters include a cryptographic key, two

1 coefficients of a linear random number generator, and an initial
2 value of the random number generator.

3 Each value, or group of values, of the robust random sequence is
4 associated with one of the pixels of the digitized image. Most
5 often the values of the random sequence are linearly remapped to
6 meet particular criteria. All the brightness values of the
7 plurality of color planes of each pixel are multiplied by its
8 associated linearly remapped robust random sequence value called
9 its brightness multiplying factor or multiplying factor. A
10 brightness multiplying factor which modifies pixel brightness
11 values by less than ten percent is herein referred to as a
12 brightness multiplying factor producing a relatively invisible
13 watermark. It is noted that depending on the texture of the image
14 being watermarked, the brightness values are generally modified
15 on average by a percentage factor of only 0.3 to 4 percent, and
16 rarely up to 10 percent. This is in order to make the marking
17 less visible. The percentage factor is herein referred to as the
18 modulation strength. The actual modulation strength employed is
19 dependent upon the classification level of invisibility required
20 by the particular use. It is not advisable to employ a brightness
21 multiplying factor greater than unity. This can result in some
22 pixel brightness values being greater than one. If employed, it
23 is recommended that all brightness values greater than one be
24 clipped to a value of unity. This can alter the pixel's color,
25 thus altering the appearance of the image.

26 Imparting a watermark upon a digitized image by varying the
27 brightness of each pixel with a multiplying factor maintains each
28 pixel's color by satisfying Grassmann's law. A compromise is
29 generally made in selecting modulation strength. A smaller

1 percentage makes the watermark less visible but more difficult to
2 detect. A larger percentage makes it easier to detect and
3 demonstrate the existence of the watermark, but makes the
4 watermark more visible. A highly textured image may require the
5 use of a relatively high modulation strength. An imparted
6 watermark is considered to be undetectably invisible in all cases
7 if the modulation strength is less than 0.5 percent, even when
8 the unmarked digitized image is a uniform medium gray. For
9 digitized images having more practical and valuable features,
10 subliminally invisible watermarks generally have modulation
11 strengths of 1% to 3%, depending on the degree of textural
12 variation in the image itself.

13 The watermark imparted in accordance with this invention is
14 selected so as to appear to be relatively invisible to any person
15 having normal or corrected visual accommodation. The probability
16 of a false-positive detection of the watermark in an image when
17 it does not exist is less than one in a million. It is possible
18 to vary the degree of imparted watermarking onto the image so
19 that the watermark can be made as detectable as necessary
20 consistent with a required invisibility classification. The
21 detected watermark is translatable to a recognizable visual
22 image, called a visualizer, having relatively bold features and
23 with a very high contrast ratio. The watermark once imparted, is
24 very difficult to remove or to be rendered undetectable without
25 reducing the usefulness and/or value of the digitized image.

26 In an embodiment of this invention, marking a digitized image
27 with an invisible watermark requires the formation of a plane for
28 watermarking. The invisible watermark is herein represented as a
29 rectangular array of numeric elements, henceforth referred to as

1 the *watermarking plane*, having I rows and J columns. The I rows
2 and J columns correspond to the dimensions of the entire original
3 digitized image, or a portion thereof, to which it is being
4 applied.

5 When an original digitized image is very large, a generated
6 watermarking plane not large enough to cover the entire original
7 image is extended by tiling replication in any direction
8 necessary to cover the entire image. If a watermarking plane
9 being so tiled extends beyond any edge of the original image, the
10 watermarking plane is assumed to be truncated. These conventions
11 are adopted for this embodiment to allow every pixel of the
12 original image to have its brightness altered and to ensure that
13 the marked image is equal in size to the original image. This
14 forms a one-to-one correspondence between element locations in
15 the watermarking plane and color components in the color planes
16 of the original image. This is generally a desirable
17 implementation, even though alternate embodiments do not require
18 watermarking the entire image.

19 In a preferred embodiment, the value of each element in the array
20 defining the watermarking plane is linearly remapped to be a
21 random number in the range,

$$1 \geq w(i,j) \geq (1 - 2\beta), \quad (1)$$

23 where,

$$1 \leq i \leq I, \text{ and} \quad (2)$$

$$1 \leq j \leq J, \quad (3)$$

are the row and column indices of the array, and β is the modulation strength of the watermark such that,

$$0.5 \geq \beta \geq 0. \quad (4)$$

Additionally, all elements in the generated watermarking plane, treated as an ensemble, are adjusted to have a mean and median of $1-\beta$.

Imparting the watermark onto an image begins with generation of this watermarking plane. The watermark is imparted onto the original image by multiplying all the brightness values associated with every pixel in each color plane by the value in its corresponding element in the watermarking plane.

CONSTRUCTING THE WATERMARKING PLANE

The construction of the watermarking plane is fundamental to insuring the robustness of the imparted watermark and its ability to survive even determined attacks. To this end, the procedure by which the values of the watermarking plane elements are chosen is based on cryptographic and two-dimensional signal processing theory techniques. These are used to satisfy particular requisite properties of the watermarking plane.

The Property of Unpredictable Randomness

Consideration is now given to the values of the watermarking plane elements to meet the property of unpredictable randomness. Unpredictable randomness requires that each element's value

1 should vary randomly from the values of its neighbors, and the
2 sequence of element values should be essentially unpredictable.
3 Random variation of the elements is required for the watermark to
4 be rendered relatively invisible. In as much as pattern
5 recognition is one of the most dominant characteristics of the
6 human visual system, the presence of any pattern among elements
7 of the watermarking plane could make it visible. The
8 unpredictability of the sequence of values is required to make
9 the watermark robust and less vulnerable to attack. It is
10 recognized that if all values in the watermarking plane could be
11 predicted, the watermarking process could easily be reversed and
12 the mark removed. This could thereby be used to essentially
13 restore the marked image to a nearly perfect copy of the original
14 unmarked image. Thus, a means of generating a highly
15 unpredictable random number sequence is preferred.

16 Generating random values by a congruence method, typical of
17 nearly all popular pseudo-random number generating algorithms, is
18 not considered herein to provide an adequate level of
19 unpredictability. These sequences have only modest cryptographic
20 strength and are relatively easily discernible by crypto-analytic
21 techniques. This is described in "The Cryptographic Security of
22 Truncated Linearly Related Variables," J. Hastad and A. Shamir,
23 Proceedings of the 17th Annual ACM Symposium on the Theory of
24 Computing, 1985, pp 356-.362, which is herein incorporated by
25 reference.

26 For the purposes of this invention a sequence is generated by
27 using a strong cryptographic method such as the National Standard
28 Data Encryption Algorithm. This is described in: "American
29 National Standard Data Encryption Algorithm," ANSI X3.92-.1981,

1 American National Standards Institute, New York; and in A. G.
2 Konheim, et al., "The IPS Cryptographic Programs," IBM System
3 Journal, Vol. 19, No. 2, 1980, pp 253-283; which are herein
4 incorporated by reference.

5 The data sequence of eight-bit values to be encrypted is selected
6 by the marker, and is desirably generated by a congruence
7 algorithm. However, the robust secure sequence is produced by
8 action of the strong encryption algorithm on that data. Using
9 this approach, a highly unpredictable watermarking plane can be
10 produced. Moreover, it can be reproduced exactly by knowing only
11 its four 'robust-watermarking-parameters'. These parameters are
12 the initial state and the two coefficients of the congruence
13 algorithm, and the cryptographic key used by the encryption
14 algorithm. These algorithms generally produce sequences of values
15 having eight-bits. Sixteen-bit values, referred to as $\alpha(i,j)$,
16 are generated by concatenating two of the sequential eight-bit
17 values produced by the encryption algorithm. Each sixteen-bit
18 value so produced is linearly remapped to become an element of
19 the array defining the watermarking plane as follows:

$$w(i,j) = 1 - 2\beta[1 - \alpha(i,j)/65535] \quad (5)$$

21 Additionally, all elements in the $w(i,j)$ array, treated as an
22 ensemble, are adjusted to have both a mean and median of $1-\beta$.
23 Ease of reproduction of the resulting encrypted sequence is
24 important for watermark detection and demonstration techniques
25 discussed subsequently. Other remapping or normalization
26 techniques producing particular desired results are known to
27 those familiar with the art.

The Property of Explicit Low Frequency Content

Another important consideration is for an embodiment that exploits the property of explicit low frequency content. Significant high frequency content results when the watermarking plane is composed by placing a unique random value in every element. Although high frequency content is beneficial in making the watermark less visible, it also makes it vulnerable to attack for watermark damage or extinction. This is evident from the following consideration. The highest pattern frequency achievable in a digitized image is obtained by replicating a pair of adjacent pixels that have opposite extreme values. When the image is reduced in size, if image reduction filtering is used, the values of adjacent pixels are combined in a weighted average to form pixel values of the reduced image. If image decimation is used, pixels are selectively discarded. In either event, the high frequency content in the original image is lost in the reduced image. Any significant high frequency content in the applied watermarking plane becomes obliterated in the reduced image. Subsequent detection of the watermark imparted prior to the size reduction is very difficult if not impossible. The purposeful addition of low frequency content makes the watermark less vulnerable to this type of attack. However, the deliberate inclusion of significant low frequency content in the watermarking plane is another dichotomy. Its inclusion indeed makes the watermark less vulnerable to normal image manipulation and therefore more easily detectable. However, it generally makes the watermark more visible by producing a pattern with larger features in the watermarking plane. It is generally preferable to add only a controlled amount of low frequency content.

1 The deliberate addition of low frequency content to the original
2 watermarking plane is accomplished in one embodiment by employing
3 the two-dimensional discrete Fourier transform. First, a
4 reduced-size watermarking plane is formed whose elements are
5 uniformly distributed random values in accordance with the secure
6 sequence described above. For discussion purposes, a square plane
7 $w(\mu, \nu)$ having $0 \leq \mu \leq \Lambda - 1$ rows and $0 \leq \nu \leq \Lambda - 1$ columns is used. The
8 discrete Fourier transform of the square plane is computed. Since
9 all values of $w(\mu, \nu)$ are real numbers, advantage can be taken
10 from the complex-conjugate symmetry of its Fourier transform. The
11 complete Fourier transform can be specified as the array of
12 complex numbers $W(\sigma, \tau)$ having dimensions $0 \leq \sigma \leq \Lambda - 1$ and $0 \leq \tau \leq \Lambda / 2$, and
13 is symbolized as:

$$W(\sigma, \tau) = \mathbf{F}[w(\mu, \nu)] \quad (6)$$

14
15
16 The frequency domain array $W(\sigma, \tau)$ is remapped into an expanded
17 array $W(s, t)$, where:

$$0 \leq s \leq L - 1, \quad 0 \leq t \leq L / 2, \quad \text{and} \quad L = 2^p \Lambda,$$

18
19 thus enlarging the (σ, τ) -space by the factor 2^p in each dimension
20 forming the larger (s, t) -space. If $W(\sigma, \tau)$ is defined such that
21 $W(0, 0)$ is the coefficient of the constant or "zero-frequency"
22 term, then:

$$W(L - s, t) = W(\Lambda - \sigma, \tau), \quad (7)$$

23
24 and

$$W(s, t) = W(\sigma, \tau), \quad (8)$$

for

$$0 \leq s = \sigma < \Lambda/2 \text{ and } 0 \leq t = \tau < \Lambda/2, \quad (9)$$

and

$$W(s, t) = 0 \quad (10)$$

for all other values of s and t . This technique is herein referred to as "zero-padding."

The inverse Fourier transform of $W(s, t)$ provides the modified watermarking plane $w(m, n)$ having $0 \leq m \leq L-1$ rows and $0 \leq n \leq L-1$ columns. If, for example, $p = 2$ and $\Lambda = 512$, then $w(m, n)$ is a square array having 2048 rows and columns. More importantly, however, $w(m, n)$ has an assured low frequency content with a minimum period ($2^p = 2^2 = 4$) four times longer than the minimum period possible in a 2048^2 image plane. Since its generating kernel, $w(\mu, \nu)$, contains 262,144 random values taken from a secure sequence, its vulnerability to attack by brute force replication is relatively small. In a case where a thus marked image appears to be vulnerable, its kernel can easily be made larger. Still lower frequency content can be impressed by using a $p=3$, making the highest frequency to be one eighth of the original highest frequency. The preferred embodiment uses $p=2$ so as not to over employ low frequency content that may cause the watermark to become undesirably visible.

The values of some elements of the generated watermarking plane so far produced may exceed one. Since each value is to be used as a multiplier of pixel brightness, it is therefore possible to

1 produce a multiplied pixel brightness that is greater than one
2 [i.e. greater than a maximum brightness], which is a brightness
3 that can not physically be displayed. In this event, any
4 multiplied pixel brightness greater than one would have to be
5 clipped to the maximum that can be displayed. The preferred
6 embodiment, however, employs an additional process step to avoid
7 the possible need for clipping. Before the generated modified
8 watermarking plane is used, its elements, forming an ensemble,
9 are adjusted to make both their mean and median values equal to
10 $1-\beta$ and the maximum value equal to 1. With these adjustments, the
11 requirement that,

$$1 \geq w(i,j) \geq (1-2\beta), \quad (11)$$

12 for all i and j is satisfied.

13
14 At this point, it is sometimes advantageous to "hard clip" the
15 elements. In this situation, elements with values greater than or
16 equal to $1-\beta$ are set to 1, and elements with values less than $1-\beta$
17 are set to $1-2\beta$. Hard clipping normally increases the probability
18 of detecting a watermark, but unfortunately, it also tends to
19 make watermarking artifacts more visible in the marked image.
20

21 **The Property of Plane Expansion by Tiling**

22 The fact that the watermarking plane $w(m,n)$ is produced as the
23 result of an inverse discrete Fourier transform is very useful.
24 If the watermarking plane is not large enough to cover the entire
25 unmarked image, if $L < I$ or $L < J$, it can be enlarged seamlessly by
26 tiling replication downward or to the right to make a plane as

1 large as desired, with each tiled extension adding an additional
2 4,194,304 elements. For the example dimensions used here, tiling
3 replication is:

$$4 \quad w(m', n') = w(m, n), \quad (12)$$

5 where,

$$6 \quad m' = (2048p) + m, \quad (13)$$

$$7 \quad n' = (2048q) + n, \quad (14)$$

8 and p and q are non negative integers.

9 In one embodiment, a watermarking plane is formed following the
10 steps 202-216 shown in Figure 2. These steps are herein referred
11 to as the 'ideal interpolator watermarking plane generating
12 method'. Firstly, an eight-bit pseudo-random sequence is
13 generated, 202. The resulting sequence is encrypted to form a
14 secure sequence of eight-bits values, 204. Sixteen bit integer
15 samples are formed by concatenating two abutted values from the
16 secure sequence, 206. The sixteen bit integer samples are
17 linearly remapped and formed into a $w(\mu, \nu)$ array such that,

$$18 \quad 1 \geq w(\mu, \nu) \geq (1 - 2\beta), \quad (15)$$

19
20 208. The discrete Fourier transform frequency domain array $W(\sigma, \tau)$
21 is computed from $w(\mu, \nu)$, 210. The $W(\sigma, \tau)$ coordinates are expanded
22 by zero-padding to form expanded frequency domain array $W(s, t)$,
23 212. The preliminary watermarking plane array $w(m, n)$ is computed
24 by taking the inverse discrete Fourier transform of $W(s, t)$, 214.
25 The elements of the preliminary array $w(m, n)$ are adjusted to

1 collectively have a mean and median of $(1-\beta)$ and a maximum of 1,
2 216a. Alternatively, the elements $w(m,n)$ are hard clipped to have
3 only values of 1 or $1-2\beta$, with a median of $1-\beta$, 216b. The
4 resulting adjusted array $w(m,n)$ is the watermarking plane with
5 elements that are brightness multiplying factors to be used for
6 adjusting corresponding pixels of the image being watermarked.

7 The method presented here, employing forward and inverse discrete
8 Fourier transforms to generate the watermarking plane, is an
9 "ideal interpolator" with assured low frequency content. Other
10 methods known to those skilled in-the-art are available. These
11 include methods that use two-dimensional interpolation filters
12 that can similarly be employed to produce acceptable results.

13 The generated watermarking plane is then imparted onto the
14 original unmarked digitized image. Figure 3 shows an embodiment
15 for the steps of watermark imparting. First, the watermarking
16 plane is expanded by tiling to completely cover the image being
17 watermarked, 302. This forms a one-to-one correspondence of an
18 element in the expanded watermarking plane and a pixel in the
19 original image. The brightness values of each pixel in the
20 original image are multiplied by the value in its corresponding
21 element in the expanded watermarking plane, 304. The resulting
22 image with the new brightness values forms the watermarked image.
23 The relative visibility of the watermark in the image is observed
24 in relationship to the desired visibility classification level
25 marking. If the marking is more visible than specified the steps
26 of Figures 2 and 3 are repeated for a lower modulation strength.
27 A watermark created with a lower modulation strength is generally
28 less easily detected and demonstrated to exist. One the other

1 hand, if the resulting watermark is less visible than specified,
2 the steps of Figures 2 and 3 may be repeated to provide a
3 watermark with a higher modulation strength. A watermark created
4 at a higher modulation strength is generally easier to detect and
5 have its existence demonstrated. Once imparted, an invisible
6 watermark only serves its purpose if it can be detected and shown
7 to exist.

8 FINDING AN INVISIBLE WATERMARK HIDDEN IN A MARKED IMAGE

9 It is most desirable to demonstrate the existence of the
10 watermark with a visible image having bold features. This is
11 herein employed using an image array called a "visualizer."
12 Demonstration of the existence of the watermark imparted in
13 accordance with the present invention requires a regeneration of
14 the watermarking plane with which it was marked. This can
15 generally only be performed by the marker and/or marking entity
16 who alone knows the four parameters making up this application's
17 "robust-watermarking-parameters". Knowledge of these parameters
18 is required for generating the robust random sequence used in
19 forming the watermarking plane. From these four parameters the
20 robust random sequence is reformed. Values of the sequence are
21 used to define the values of the elements. If a linear remapping
22 process was employed in the generation of the watermarking plane,
23 the element values are linearly remapped using that same process
24 to redefine the expanded watermarking plane. The thus reformed
25 expanded watermarking plane is used in conjunction with the
26 visualizer to demonstrate the existence of the expanded
27 watermarking plane in the image. This is accomplished as
28 described subsequent to an overview of watermark detection
29 considerations.

1 Finding an invisible watermark hidden in a marked digitized image
2 is a relatively difficult problem, and it is made more so by
3 manipulations of the marked image that may have occurred. The
4 watermark survives and is detectable for image manipulations that
5 in themselves do not damage the image beyond usability. The
6 detection method of the present invention can find an imparted
7 watermark with a high degree of certainty in nearly all such
8 cases. A significant advantage of the present method is that
9 watermark detection does not require access to a copy of the
10 entire original image. In most cases, all that is required is the
11 watermarking plane used for imparting the watermark on the image.
12 A perfect copy of the watermarking plane is reconstituted from
13 its four defining parameters. If a copy or if even only a
14 fragment of the original image is available, detection can have a
15 somewhat higher probability of success.

16 **Reorienting and Resizing the Watermarking Plane**

17 A first consideration in finding a watermark is to determine how
18 and by how much the marked image may have been manipulated. It
19 may have been reduced in size. A size reduction may even have
20 been performed nonlinearly, such that its horizontal and vertical
21 dimensions may have been reduced by unequal factors. The image
22 may also have been rotated, not by an obvious ninety degrees, but
23 by a small angle. Facilitating this determination is the
24 knowledge that pixel values in the unmanipulated marked image are
25 directly related to corresponding elements in the watermarking
26 plane. If a significant fragment of the original image is
27 available, a fragment of the unmanipulated marked image can be
28 reconstructed. Either the reconstituted watermarking plane or a

1 reconstructed fragment of the marked image is a suitable
2 "correlation reference plane."

3 An overview of the steps of reconstructing a manipulated
4 watermarked image is shown in Figure 4. First, the watermarking
5 plane used for imparting the watermark onto the image is
6 regenerated from the four 'robust-watermarking-parameters'
7 generally only known to the marker and/or the marking entity,
8 402. Secondly, the marked image is resized and rotated to its
9 known original dimensions, 404. Thirdly, the resized and rotated
10 image is aligned with the expanded regenerated watermarking plane
11 such as to provide one-to-one correspondence of the elements of
12 each with the elements of the other, 406.

13 In an actual implementation the steps of reorienting and resizing
14 the marked image may be broken into a coarse placement followed
15 by a fine alignment. The coarse placement is performed by visual
16 inspection of a displayed copy of a portion or the complete
17 marked image overlaying a corresponding portion or complete
18 correlation reference plane. The correlation reference plane is
19 reoriented and resized to the size and orientation of the marked
20 image by axis reduction or expansion, translation and/or
21 rotation. This is accomplished using techniques well known to
22 those skilled in the art. The coarse placement generally brings
23 the correlation reference plane to within 4 percent of the
24 manipulated marked image's size and within four degrees of its
25 orientation.

26 Figure 5 shows the steps for an embodiment for performing coarse
27 placement. Both the marked image and the correlation reference
28 plane are displayed on a common display, 502. The vertical axis

1 and horizontal axis magnification, offset and angular rotation of
2 the correlation reference plane display are varied to make the
3 displayed correlation reference plane closely overlay the
4 corresponding portions of the displayed manipulated marked image,
5 504. The values of the magnification/reduction factors,
6 horizontal and vertical offsets and angle of rotation are noted
7 and stored, 506. The entire marked image is rescaled, translated
8 and rotated by the inverses of the noted values so that it
9 visually matches the correlation reference plane, 508. The so
10 coarsely manipulated reconstituted marked image is further
11 manipulated to perform the fine alignment.

12 According to the Fourier Shift Theorem, Rotation Theorem and
13 Scaling Theorem, the properties of translation, rotation and
14 scaling transcend the Fourier transformation of an image, and, if
15 present in $w(m,n)$, each will also be present (or, in the case of
16 scaling, its reciprocal will be present) in $W(s,t)$. This is
17 useful to determine a more precise angle of rotation, horizontal
18 and vertical scale factors, and translation offsets of the
19 correlation reference plane relative to the marked image. This is
20 accomplished by first constructing a three-dimensional "array of
21 phase-correlation maxima." The three axes of the array correspond
22 to the horizontal scale factor, the vertical scale factor, and
23 the angle of rotation of the correlation reference plane relative
24 to the marked image. Phase-correlation is defined as follows. Let
25 $W(s,t)$ be the discrete Fourier transform of the correlation
26 reference plane, $U(s,t)$ be the discrete Fourier transform of the
27 marked image $u(m,n)$, and $U^*(s,t)$ be the complex conjugate of
28 $U(s,t)$. The phase-correlation plane $p(m,n)$ is computed using the
29 relationship:

$$p(m,n) = F^{-1} \left[\frac{W(s,t)U^*(s,t)}{|W(s,t)U^*(s,t)|} \right]. \quad (16)$$

The value at each array point is the maximum magnitude of the corresponding phase-correlation plane. It is computed using an incrementally rescaled and rotated correlation reference plane. Any one of the color planes of the marked image usually suffices as the required array $u(m,n)$. Interpolating among the values of the three-dimensional array yields coordinates of the greatest-of-the-greatest phase-correlation maxima. From these coordinates, values of the horizontal and vertical scale factors and angle of rotation of the correlation reference plane relative to the marked image are directly read. The correlation reference plane is then rescaled and rotated to more precisely align it with the manipulated marked image. A final phase-correlation evaluation is made to determine the relative horizontal and vertical offsets of the modified correlation reference plane relative to the manipulated marked image. Finally, the entire marked image is rescaled, translated and rotated in accordance with the inverses of the measured values to restore it to its original size and orientation. The thus modified marked image is now ready for use in the detection and demonstration process to show the existence of the watermark in the manipulated marked image.

In one embodiment the fine alignment of the correlation reference plane relative to the marked image is performed by evaluating a three-dimensional array of phase-correlation maxima, and then interpolating within that array to find the location of the maximum of those maxima. The axes of the array are the horizontal magnification, vertical magnification and angular rotation that

1 are systematically applied to the correlation reference plane.
2 All combinations of the following incremental steps define the
3 values of the coordinates of the array. The vertical axis of
4 $w(m,n)$ is magnified/reduced from 96% to 104% of its original size
5 in 2% increments. In similar fashion the horizontal axis of
6 $w(m,n)$ is magnified/reduced from 96% to 104% of its original size
7 in 2% increments. Also in similar fashion $w(m,n)$ is rotated
8 relative to its original orientation from -5 degrees to +5
9 degrees in 2 degree steps. At each combination of vertical
10 magnification, horizontal magnification, and angular rotation of
11 the correlation reference plane, the phase-correlation plane
12 $p(m,n)$ is recomputed as above. The maximum of the point values
13 $p(m^*,n^*)$ in the plane is stored into the three-dimensional array
14 of phase-correlation maxima at coordinates corresponding to each
15 of the incrementally adjusted values of vertical magnification,
16 horizontal magnification, and angular rotation.

17 A flow diagram of this embodiment is shown in Figure 6. Those
18 skilled in the art know there are many satisfactory algorithms
19 available to magnify/reduce and rotate digitized images. Any one
20 of those algorithms can be used for manipulation of the
21 correlation reference plane in the following description. As
22 described above, the discrete Fourier transform of the marked
23 image $U(s,t)$ is formed, 602. Initial values are set for stepping
24 variables vertical magnification, $V_m=0.96$, horizontal
25 magnification, $H_m=0.96$, and angular rotation, $A_r=-5^\circ$, 604. The
26 correlation reference plane is vertically magnified/reduced
27 according to V_m , 606. The so adjusted plane is then horizontally
28 magnified/reduced according to H_m , 608. The so adjusted plane is
29 then rotated according to A_r , 609. The discrete Fourier transform
30 of the so adjusted plane $W(s,t)$ is formed, 610. The

1 phase-correlation plane $p(m,n)$ is calculated using the
2 relationship of equation (16), 611. The $p(m,n)$ plane is examined
3 to find the coordinates (m^*,n^*) of its maximum value, 612. The
4 coordinates (m^*,n^*) and $p(m^*,n^*)$ are stored in the
5 three-dimensional array being formed. The three-dimensional array
6 is indexed by V_m , H_m and A_r , 613. The value of A_r is examined,
7 614. If it is less than plus five degrees, it is incremented by
8 plus two degrees, 615, and steps 609-614 are repeated until A_r is
9 found to be plus five degrees in step 614. When A_r is found to be
10 plus five degrees in step 614, the value of H_m is examined, 616.
11 If H_m is less than 1.04, it is incremented by 0.02 and A_r is
12 reinitialized to minus five degrees, 617. Steps 608 to 616 are
13 repeated until H_m is found to be 1.04 in step 616. When H_m is
14 found to be 1.04, V_m is examined, 618. If V_m is found to be less
15 than 1.04, it is incremented by 0.02, and A_r is initialized to
16 minus five degrees, and H_m is initialized to 0.96, 619. Steps 606
17 to 618 are repeated until V_m is found to have a value of 1.04 in
18 step 618. When V_m is found to be equal to 1.04, the values of the
19 three-dimensional array are interpolated to find the maximum of
20 the maxima peaks, 620. The resulting coordinates of the maximum
21 of maxima peaks provide the final values for the vertical
22 multiplier, the horizontal multiplier and the rotational angle
23 for best alignment of the manipulated marked image with the
24 correlation reference plane. The corresponding resulting values
25 of m^* and n^* of the maximum of maxima provide the offset
26 displacements of the manipulated marked image relative to the
27 correlation reference plane. The manipulated marked image is then
28 rescaled by the inverses (reciprocals) of the found vertical and
29 horizontal multipliers. It is rotated by the inverse (negative)
30 of the found angular rotation, and is offset by the inverses

1 (negatives) of m^* and n^* , 622. This completes the fine setting
2 process of reorienting and resizing.

3 It will be apparent to those skilled in the art that either the
4 correlation reference plane or the manipulated marked image can
5 be resized and reoriented to bring one into alignment with the
6 other. The preferred embodiment resizes and reorients the
7 manipulated marked image to bring it into alignment with the
8 correlation reference plane, and hence into element-to-element
9 alignment with the watermarking plane.

10 **Detecting the Watermark in a Marked Image**

11 The process of watermark detection is designed to produce a
12 visibly recognizable small image as its end product. The
13 recognizable end product is obtained in a procedure which depends
14 upon the existence and knowledge of the watermark based on the
15 robust random sequence. The process exploits the extremely
16 sophisticated and not yet completely understood pattern
17 recognition capabilities of the human visual system. It is
18 through this exploitation that defeating the imparted watermark
19 becomes much more difficult. A small rectangular array, called a
20 selector, is conceived to implement the detection process. The
21 selector array size must be much smaller than the pixel array of
22 the marked image to which it is being applied. This is to allow
23 overlaying the selector on the image hundreds of times without
24 overlapping. The selector array should be made large enough that
25 a pixel array having the same dimensions could contain a
26 recognizable binary image. More complex embodiments use a color
27 rather than binary image as a reference. A selector having 32
28 rows and 128 columns is used in an embodiment described herein.

1 It is applied to a marked image that has more than one million
2 pixels.

3 The selector is used to locate rectangular clusters of pixels in
4 the marked image and corresponding clusters of elements in the
5 reconstituted watermarking plane. The clusters are randomly
6 scattered non-overlapping positions. Random scattering of the
7 clusters is done to further frustrate attempts to defeat
8 watermark protection. Each element of the selector contains one
9 or more devices associated with variables that serve to store
10 partial results of the watermark detection scheme. One embodiment
11 uses two selector devices, one called a "coincidence counter" and
12 the other a "non-coincidence counter." All coincidence counters
13 and non-coincidence counters are set to a zero value before the
14 detection process is begun.

15 A variable, called a *statistically related variable*, is defined
16 which statistically relates an attribute of an element being
17 considered to the attributes of its neighboring elements. For
18 each pixel in the marked image a first variable is computed for
19 that pixel and a second variable is computed for that pixel's
20 corresponding element in the reconstituted watermarking plane. A
21 positive test results when the computed first variable has the
22 same result, or a nearly or statistically deemed equivalent
23 result, as the computed second variable. If the results are
24 deemed to be different, the test result is deemed to be negative.
25 The first variable is recomputed and compared with the second
26 variable for each of that pixel's color planes. The coincidence
27 counter associated with that selector element is incremented by
28 unity for each color plane producing a positive result and the
29 non-coincidence counter is incremented by unity for each color

1 plane that produces a negative result. The purpose of each
2 element's coincidence and non-coincidence counters is to
3 associate with that element a confidence level of the watermark's
4 identification with the random sequence known only to the marker
5 and/or the marking entity. The quantified confidence level for
6 each element is derived from the values in that element's
7 coincidence and non-coincidence counters, and is called a
8 coincidence value.

9 For a tristimulus color image and for each cluster of pixels, the
10 range of each coincidence counter value is from zero to plus
11 three. A zero is obtained if the test results were negative for
12 all three color planes. A plus three is obtained if the test
13 results were positive for all three planes. The range of each
14 non-coincidence counter is also from zero to plus three, but
15 conversely, a zero is obtained if the test results for all three
16 planes were positive and a plus three is obtained if the test
17 results of all three planes were negative. The count in each
18 coincidence counter is the accumulated sum of the counts of
19 positive results for corresponding pixels at each cluster
20 location, and the count in each non-coincidence counter is the
21 accumulated sum of the counts of negative results for
22 corresponding pixels at each cluster location. A coincidence
23 counter value larger than the value of its corresponding
24 non-coincidence counter is associated with a partial watermark
25 detection. A composite of coincidence counter values greater than
26 their corresponding non-coincidence counter values for a
27 preponderance of the selector's elements results from and
28 corresponds with a detected watermark having a high confidence
29 value.

1 In an embodiment the test results and/or the comparison are
2 performed by subtraction operations. In a particular embodiment
3 the attribute used is the pixel's brightness values. The
4 statistical relationship is in regard to the average brightness
5 value of the neighboring pixels. In this case, watermark
6 detection proceeds with the steps shown in Figure 7. A selector
7 array size is selected, 702. In this example, the selector array
8 size is 32 by 128 elements. All the coincidence and
9 non-coincidence counters are initialized by setting them to read
10 zero, 704. A specified particular element of the selector is
11 placed on an initial position of the expanded watermarking plane,
12 706. The particular first element is often the selector element
13 that is at its upper leftmost corner. This particular element
14 also locates a corresponding pixel and its components in all the
15 color planes of the marked image when the marked image is aligned
16 with the expanded watermarking plane.

17 The following portion of the detection schema is repeated
18 iteratively for all selector elements, for all color planes of
19 each pixel, and for all selected clusters. The next two eight-bit
20 integers are chosen from the regenerated robust random sequence,
21 708. When the schema is started for the first selector element,
22 the next two eight-bit integers chosen in this step 708 are
23 actually the first two eight-bit integers of the robust random
24 sequence. The two eight-bit integers are scaled to form random
25 horizontal and vertical offsets from the initial or previous
26 selector location, and the selector is moved to that position,
27 710. The selector element sequence is reset to the coordinates of
28 the initial particular selector element, 711. This selector
29 element is used to locate the corresponding particular element in
30 the watermarking plane, 712. The average magnitude of its

1 neighboring elements in the watermarking plane is computed, 713.
2 In the example, this is the average of the magnitudes of the
3 particular element's neighbors that lie in an 11 by 11 square of
4 elements with the particular element at the center of the square.
5 If the selector element is too near an edge of the watermarking
6 plane to be at the center of its neighborhood, the square
7 neighborhood is moved to encompass the particular element's
8 nearest 120 existing neighbors.

9 The next color plane is chosen, 714. In the beginning of this
10 iterative schema this next color plane is actually the first
11 color plane. In the case of a monochrome image this is the only
12 color plane. The coordinates of the particular selector element
13 are used to locate a corresponding pixel color component in this
14 next color plane, 715. The average brightness of the neighboring
15 120 pixel color components is computed, 716, in a manner
16 identical to that stated above for watermarking plane elements.
17 The values of the particular watermarking plane element and the
18 corresponding pixel color component are compared to their
19 respective neighborhood averages. If both values are equal to or
20 greater than their respective neighborhood averages, 717, or if
21 both values are less than their respective neighborhood averages,
22 718, the coincidence counter of that particular selector element
23 is incremented, 719a. If one value is less than its respective
24 neighborhood average and the other value is equal to or greater
25 than its respective neighborhood average, the non-coincidence
26 counter of that particular selector element is incremented, 719b.
27 The magnitude of the value in each coincidence counter relative
28 to the magnitude of the value in its corresponding
29 non-coincidence counter is associated with the probability of
30 watermark sequence validation.

1 A determination is made if all color planes were chosen for
2 testing their corresponding brightness value with regard to its
3 neighboring average, 720. If not, the process returns to step 714
4 for choosing the next color plane. Steps 715 to 720 are repeated
5 for this color plane. This is continued until step 720 indicates
6 the all color planes are tested. When the last (or only)
7 color-plane is tested, a determination is made if every element
8 for that selector was chosen, 724. If not, the next selector
9 element is chosen, 726. Generally, the next element is the next
10 right-wise adjacent element on that row. If there is no next
11 adjacent element on that row, the next element is the left-most
12 element in the next selector row. This next selector element
13 becomes the new particular element. Steps 712-724 are repeated
14 until all selector elements are chosen and tested. When it is
15 determined in step 724 that all elements have been chosen, a
16 determination is made if all non-overlapping selector locations
17 have been chosen, 728. If not, steps 708 through 728 are repeated
18 for all selector elements and marked image color planes. When it
19 is determined in step 728 that all selector locations are tested,
20 all coincidence counters have their test result values.

21 Figure 8 shows a random multiple totality of positions of the
22 selector 810 in a selector plane 802 resulting from an
23 implementation of the process of Figure 7. Figure 8 shows a
24 watermarking plane 804 and three color planes 806-808 of the
25 marked image. The first selector element acted upon is often the
26 top leftmost element 812 of the selector in each of the selector
27 positions. It is noted that although each selector position is
28 randomly offset from previously chosen positions, the positions
29 do not overlap each other.

1 The values contained within each coincidence and non-coincidence
2 counter associates with their corresponding selector element a
3 confidence level of the watermark's identification with the
4 random sequence known only to the marker and/or the marking
5 entity. The watermark is considered to be detected if a
6 preponderance of the differences of coincidence counter values
7 less their respective non-coincidence counter values are non
8 negative. Thus, an examination of the totality of these non
9 negative differences explicitly suffices for declaring the
10 watermark detected or not detected. Indeed, this can be
11 considered as the end of the watermark detection technique.

12 Those skilled in the art will recognize that it is possible to
13 mathematically derive a "probability of watermark detection," in
14 which the "probability of watermark detection" is greater than
15 zero and less than one (where a value zero represents certainty
16 of the absence of a watermark and a value one represents
17 certainty of its presence), based only on the coincidence and
18 non-coincidence counter values and assuming only the property of
19 uniform distribution of the random brightness multiplying
20 factors. However, alternative embodiments recognize that a
21 "preponderance" of differences being non negative is an inexact
22 measure, at best. Clearly, if only a simple majority of the
23 differences are non negative, whether the watermark is detected
24 or not is at best a judgment call. Most likely it would be
25 conceded as not having been a detection. To assist in this
26 judgment, the present invention exploits the ability of the human
27 visual system to recognize a pattern in a cluttered field. This
28 is accomplished by forming a binary image called a visualizer.
29 The visualizer is formed to have the same dimensions as the

1 selector (e.g., 32x128 pixels). A clearly recognizable pattern is
2 placed into the visualizer. A typical visualizer pattern is shown
3 in Figure 9, 900. The black border surrounding the visualizer is
4 not considered to be part of the visualizer pattern. The pattern
5 is an arrangement of blocks of black and white pixels forming an
6 easily recognizable pattern. A typical pixel, 902, is at the
7 lower ending of the image of a C. The visualizer image is
8 entirely white except for pixels making the letters IBM, 904, the
9 copyright logo, 906, and the visualizer frame, 908.

10 The visualizer pattern is used to provide a visual image of the
11 actual degree of "preponderance" of coincidence counters being
12 non negative. The method steps diagrammed in Figure 10 are used
13 to provide a watermark signature in relation to the visualizer
14 pattern. The watermark signature is derived by using the
15 visualizer pattern in combination with the coincidence counter
16 difference data to form what is herein referred to as the
17 'visualizer-coincidence image'.

18 In one embodiment, the visualizer-coincidence image is formed
19 with the steps shown in Figure 10. A visualizer pattern is formed
20 having a pixel array equal in size to the element array of the
21 selector, 1002. The visualizer array consists of white and black
22 pixels, where white is given the value one and black the value
23 zero. All elements of the selector array will be examined to
24 determine the pixel content of the visualizer-coincidence image.
25 To do this, the selector element sequence is reset and the first
26 element of the sequence is chosen, 1004. For the chosen selector
27 element, the count in its corresponding non-coincidence counter
28 is subtracted from the count in its corresponding coincidence
29 counter, forming a difference, 1006. The sign of the difference

1 is tested, 1008, and if it is negative the corresponding pixel of
2 the visualizer is inverted (white is changed to black, and black
3 to white) and placed into the corresponding pixel of the
4 visualizer-coincidence image, 1010b. If the sign is positive, the
5 corresponding pixel of the visualizer is placed unmodified into
6 the corresponding pixel of the visualizer-coincidence image,
7 1010a. The selector element sequence is tested to see if all
8 elements have been chosen, 1012, and if not , the next element is
9 chosen, 1014, and steps 1006 to 1012 are repeated. If all
10 selector elements have been chosen, the visualizer-coincidence
11 image is displayed, 1016. A judgment is made as to whether the
12 pattern in the visualizer-coincidence image is recognized as a
13 reproduction of the visualizer pattern, 1018. If it is
14 recognized, the watermark is positively detected, 1020a. If not,
15 the watermark is not detected, 1020b.

16 It is evident to those skilled in the art that if only the sign
17 of the difference between the count in a coincidence counter less
18 the count in its corresponding non-coincidence is to be used in
19 constructing the visualizer-coincidence image, then only one
20 counter would have been needed for each selector element. In that
21 case, step 719a of Figure 7 would read "Increment the counter of
22 Selector's Element," and step 719b would read "Decrement the
23 counter of Selector's Element."

24 Figure 11 shows a detection, 1102, resulting from the visualizer
25 of Figure 8 for an imparted watermark made at a modulation
26 strength of 1%. As previously stated in all cases the black
27 border is not part of the visualizer-coincidence image. A
28 stronger replication of the visualizer, 1202, resulting for an
29 imparted watermark made at a modulation strength of 2% is shown

1 in Figure 12. A still stronger replication of the visualizer,
2 1302, resulting for an imparted watermark made at a modulation
3 strength of 4% is shown in Figure 13.

4 An attempt to detect a watermark in an image that does not have
5 one, or in an image for which the watermarking plane cannot be
6 reconstituted, produces a visualizer pattern that is an
7 unrecognizable random melee. Figure 14 shows a typical
8 visualizer-coincidence image, 1402, when a watermark is not
9 detected. This results when many visualizer pixels are subjected
10 to inversion. A preponderance of pixels not requiring inversion
11 indicates watermark detection. This method in fact has an
12 extremely low probability of false-positive detection. Even in a
13 highly textured marked image, the visualizer pattern should be
14 clearly recognizable to signify a watermark detection of very
15 high credibility.

16 Clearly, more information is present in the coincidence and
17 non-coincidence counter values than has been exploited above,
18 where only the algebraic sign of their difference has been used.
19 An alternative method of converting the visualizer image into a
20 visualizer-coincidence image uses the magnitude of each
21 coincidence counter value and that of its corresponding
22 non-coincidence counter. If $C(i',j')$ is the value of the
23 coincidence counter associated with selector element i',j' and
24 $C'(i',j')$ is the value of the corresponding non-coincidence
25 counter, then the normalized magnitude of their difference
26 $e(i',j')$ is:

$$e(i',j') = C(i',j') / [C(i',j') + C'(i',j')] \quad (17)$$

1 when $C(i',j')+C'(i',j')>0$, (18)

2 and:

3 $e(i',j') = 1/2$, (19)

4 when $C(i',j')+C'(i',j')=0$. (20)

5 In this case, the visualizer image is converted into a
6 visualizer-coincidence image by replacing each pixel in the
7 visualizer image with the corresponding value of $e(i',j')$, when
8 the visualizer pixel value is one; and by $1-e(i',j')$, when the
9 visualizer pixel value is zero. Notice that the
10 visualizer-coincidence image is no longer a binary image, but
11 includes gray shades ranging from black to white. The judgment as
12 to whether the pattern placed in the visualizer is recognizable
13 in the visualizer-coincidence image is the same as before, and an
14 attempt to detect the presence of a known watermark in an image
15 not having one, or in an image having one but for which the
16 watermarking plane cannot be precisely reconstituted, also still
17 produces an unrecognizable random melee in the
18 visualizer-coincidence image.

19 Thus, this scheme makes more use of the actual values in the
20 coincidence and non-coincidence counters. It still employs a
21 black and white element visualizer image pattern wherein each
22 element is either black or white (zero or one). However, the
23 resulting elements of the visualizer-coincidence image have
24 values ranging between zero and one such that when displayed it
25 has various levels of shades of gray. The gray level depends on
26 the counter data.

1 An embodiment of this alternative scheme is shown in Figure 15. A
2 visualizer pattern is formed having a pixel array equal in size
3 to the element array of the selector, 1502. The visualizer array
4 consists of white and black pixels, where white is given the
5 value one and black the value zero. All elements of the selector
6 array will be examined to determine the pixel content of the
7 visualizer-coincidence image. To do this, the selector element
8 sequence is reset and the first element of the sequence is
9 chosen, 1504. For the chosen selector element, the ratio of the
10 count in its corresponding coincidence counter to the sum of the
11 counts in its corresponding coincidence and non-coincidence
12 counters is computed, 1506. The color of the corresponding
13 visualizer pixel is tested, 1508, and if it is black, the ratio
14 subtracted from one is placed into the corresponding pixel of the
15 visualizer-coincidence image, 1510a. If the visualizer pixel is
16 white, the ratio is placed unmodified into the corresponding
17 pixel of the visualizer-coincidence image, 1510b. The selector
18 element sequence is tested to see if all elements have been
19 chosen, 1512, and if not, the next element is chosen, 1514, and
20 steps 1506 to 1512 are repeated. If all selector elements have
21 been chosen, the visualizer-coincidence image is displayed as a
22 high contrast monochrome image, 1516. A judgment is made as to
23 whether the pattern in the visualizer-coincidence image is
24 recognized as a reproduction of the visualizer pattern, 1518. If
25 it is recognized, the watermark is positively detected, 1520a. If
26 not, the watermark is not detected, 1520b.

27 THE IMPLEMENTATION OF BRIGHTNESS MODIFICATION BY ADDITION INSTEAD
28 OF MULTIPLICATION

1 An alternative, and equivalent, form for modifying pixel
 2 brightness is to change the brightness by adding to or
 3 subtracting from the component $Y(i,j)$ a different small random
 4 value $\varepsilon(i,j)$. As before stated, $1 \leq i \leq I$ and $1 \leq j \leq J$ are the
 5 row and column indices of the pixel location in the image. To
 6 help make the brightness variation less visible, $\varepsilon(i,j)$ is made
 7 proportional to the original brightness of the component, thereby
 8 making the change smaller in darker areas of the image where the
 9 human eye is more discerning of changes in brightness. Thus,
 10 $\varepsilon(i,j) = \delta(i,j)Y(i,j)$, where $\delta(i,j)$ is a value selected from an
 11 array of random values that may have the range $-0.5 < \delta(i,j) <$
 12 0.5 . The modified component $Y'(i,j) = Y(i,j) + \varepsilon(i,j) =$
 13 $Y(i,j) + \delta(i,j)Y(i,j)$. To alter only the brightness of each pixel
 14 in a color image, the ratios of its components must be preserved.
 15 If the color components of the unaltered pixel are $X(i,j)$,
 16 $Y(i,j)$, and $Z(i,j)$, and the color components of the brightness
 17 altered pixel are $X'(i,j)$, $Y'(i,j)$, and $Z'(i,j)$, then
 18 $X'(i,j)/X(i,j) = Z'(i,j)/Z(i,j) = Y'(i,j)/Y(i,j) = 1 + \delta(i,j)$. It
 19 is evident that this is equivalent to multiplying the brightness
 20 of the each color component by $1 + \delta(i,j)$, since $X'(i,j) =$
 21 $X(i,j)[1 + \delta(i,j)]$, $Z'(i,j) = Z(i,j)[1 + \delta(i,j)]$, and $Y'(i,j) =$
 22 $Y(i,j)[1 + \delta(i,j)]$. If the random values $1 + \delta(i,j)$ are set equal to
 23 $w(i,j)$ as defined before, the two methods are identical. In
 24 summary, the modification of pixel brightness by an additive
 25 value that is proportional to pixel brightness while preserving
 26 the ratios of the color components of the pixel is equivalent to
 27 modifying the brightness of the pixel by multiplication. An
 28 additive and multiplicative modulation can have a different

1 effect only if the ratios of the color components of the pixel
2 are allowed to change.

3 USING A BLURRING FILTER BEFORE ATTEMPTING WATERMARK DETECTION TO
4 IMPROVE THE PROBABILITY OF DETECTION

5 Watermark detection may be enhanced in accordance with the
6 present invention as described hereinafter in a manner that is
7 adaptable for use of any of many watermarking techniques. It is
8 most particularly adaptable to a watermarking technique employing
9 a watermarking plane. Thus, although the enhancement of the
10 detection technique is adaptable to many watermarking techniques,
11 it is most easily described and adaptable to the watermark
12 imparting and detecting methods described previously herein.

13 As described above for particular embodiments, watermarks are
14 imparted into an image by multiplying the components of each
15 pixel of the image by the linearly remapped values of the
16 watermarking plane, $w(i,j)$, where $1 > w(i,j) \geq (1-2\beta)$, i is the
17 value's row index, j is the value's column index, and β is the
18 modulation strength of the watermark. Additionally, all elements
19 in the generated watermarking plane, treated as an ensemble, are
20 adjusted to have a mean and median of $1-\beta$. In other watermark
21 embodiments this is accomplished by addition and/or subtraction
22 operations.

23 A method for improving the detection of the imparted watermark in
24 a marked image and, more specifically, in a derived copy of a
25 marked image employs use of a two-dimensional **blurring filter**
26 prior to an attempted detection. A blurring filter is also called

1 a low-pass filter in signal-processing terminology. Application
2 of the blurring filter is advantageous in that it reduces
3 high-frequency noise content among the color components in the
4 marked image while leaving low-frequency content relatively
5 unaltered.

6 In the example embodiment, since the watermark, as imparted into
7 the image, has the appearance and behavior of a two-dimensional
8 noise pattern itself, any addition of high-frequency noise can
9 potentially partially obscure the watermark and make it more
10 difficult to detect. This is specifically the case if a derived
11 copy is produced by scanning a printed copy of a marked image.
12 Substantial high-frequency noise is added to a marked image by
13 the screening process used in preparation for its printing.
14 Printing ordinarily is accomplished with one or several inks or
15 dyes that each have an invariable color. The screening process
16 produces various shades of the invariably colored inks or dyes,
17 needed to reproduce the color components, by covering the spatial
18 area represented by each pixel with a finer grid of dots of the
19 inks or dyes. Each of the grids of dots has a varying spatial
20 density of the inks or dyes, and each dot in a grid of dots is
21 significantly smaller spatially than the pixel area. The grids of
22 dots so produced, one for each color component, spatially replace
23 the pixel they represent in the printed image copy, and, after
24 fusion by the human viewing system, collectively produce a
25 perceived correct color of the pixel.

26 The screening process, by converting the components of each pixel
27 into grids of dots of still smaller dimensions, inherently adds
28 high-frequency artifacts and noise to the printed image copy that

1 were not in the original image. This can be verified easily by
2 viewing a printed image under moderate magnification. If the
3 printed image is then scanned to produce a derivative digitized
4 image, the added high-frequency noise reproduced in the
5 derivative copy is detrimental to watermark detection. It is to
6 reduce the detrimental effects of the added high-frequency that a
7 blurring filter is used. As stated above in the subsection titled
8 **"The Property of Explicit Low Frequency Content"** the watermarking
9 plane is designed to have significant low frequency content and
10 will thus be relatively immune to the action of a blurring
11 filter, but the high-frequency content of image, and more
12 importantly the added noise, will be substantially attenuated.

13 An example rudimentary blurring filter can be implemented in the
14 following manner. Each color plane of the image, represented as a
15 rectangular array of like color components, is partitioned, right
16 to left and top to bottom, into small sub-arrays that are three
17 pixels high and three pixels wide. If the number of pixels in a
18 row or column of the image array is not evenly divisible by
19 three, the edge sub-arrays at the right or bottom of the
20 partitioned image will contain fewer than nine pixels. The color
21 components of the nine pixels in each sub-array (or fewer than
22 nine if the sub-array is an edge sub-array) are averaged. The
23 average value of the color components in each sub-array is then
24 used to replace all the values in that sub-array. This completes
25 the two-dimensional blurring filter. Those skilled in the art
26 will recognize that there many other more sophisticated ways to
27 implement a two-dimensional blurring filter. Nevertheless, in the
28 method of the present invention the important desired result of
29 applying any blurring filter remains the same as the that of
30 applying the rudimentary filter described here, namely, the

1 reduction of high spatial frequencies and the preservation of low
2 spatial frequencies of features in the derivative image.

3 In the example rudimentary blurring filter presented, the first
4 step of the method was to divide a marked image's color plane
5 into nine element square sub-arrays. The choice of the size of
6 the sub-arrays determines the degree to which high spatial
7 frequencies among the pixel components in the marked image are
8 reduced in the filtered image, if the marked image contains such
9 high spatial frequencies, which it may not. By using nine element
10 sub-arrays, the highest spatial frequency that can possibly exist
11 in the filtered image is reduced by a factor of three. The larger
12 the sub-array is chosen, the greater is the reduction of the
13 highest possible spatial frequency that can exist in the filtered
14 image. It will be apparent to those skilled in the art that, when
15 applying a blurring filter, the degree to which the highest
16 spatial frequency is to be reduced depends upon the degree to
17 which high-frequency content in the watermarking plane used to
18 produce the marked image was reduced. If the objective of using
19 the blurring filter it to improve watermark detection, it would
20 become counter productive to reduce the high-frequency content of
21 the marked image by a factor greater than that used in creating
22 the watermarking plane; to do so would remove not only
23 undesirable high-frequency noise in the marked image but also
24 some of the information contained in the imparted watermark.

25
26 Referring to Figure 16, a highly enlarged segment of an example
27 watermarked image is shown. The watermark was imparted according
28 to the method described previously herein. The modulation
29 strength, β , used for the marking was 2.5 percent and visibility

1 of the watermark, even at high magnification is classified as
2 *undetectable invisible*. Referring to Figure 17, a similarly
3 enlarged segment of a derivative image is shown; it is derived
4 from the marked image shown in Figure 16 after it is screened in
5 preparation for printing, forming a screened image, and
6 subsequently printed and scanned. Note that significant
7 high-frequency noise resulting from the screening process is
8 evident in Figure 17. Figure 18 shows a filtered image produced
9 by applying the rudimentary blurring filter to the derived image.
10 The noise reduction resulting from application of the blurring
11 filter is evident by comparing Figure 18, after the application,
12 with Figure 17, before the application.

13 Watermark detection was attempted for each of the three images,
14 the enlarged segments of which are shown in Figures 16, 17, and
15 18. The watermark visualizer-coincidence images realized from the
16 detection using the original marked image is shown in Figure 19.
17 The detection is a perfect detection. The original marked image
18 is then screened for printing, printed and scanned to form the
19 derivative image. The watermark visualizer-coincidence image
20 realized from the detection using the derivative image is shown
21 in Figure 20. The detection is very weak, nearly nonexistent.
22 After the rudimentary blurring filter is applied to the
23 derivative image to form the filtered image, watermark detection
24 is again attempted. The watermark visualizer-coincidence image
25 realized from the detection using the filtered image is shown in
26 Figure 21. The detection, although imperfect, is very strong,
27 testifying to the efficacy of the use of the blurring filter
28 before attempting watermark detection.

1 Use of a blurring filter is advantageous before any attempted
2 watermark detection, regardless of the robust watermarking method
3 used. If a watermark is robust, that is, if it is resistant to
4 attacks, it must ordinarily contain significant low-frequency
5 content. The low-frequency content of the watermark will not be
6 unduly disturbed by the blurring filter, since the blurring
7 filter is by its nature a low-pass filter. Any
8 detection-disturbing high-frequency content in the image, whether
9 occurring naturally as a part of the image or whether added by
10 artificial means, such as screening in preparation for printing,
11 will be suppressed by the action of the blurring filter. The
12 actual amount of blurring is generally dependent upon the
13 particular application and/or watermark. This is determined in
14 ways known to those skilled in the art.

15 Although the description is made for particular embodiments,
16 techniques and arrangements, the intent and concept of the
17 present invention are suitable to other embodiments, techniques
18 and arrangements. For example, an obvious choice, and the choice
19 of last resort, in demonstrating the existence of a watermark in
20 a manipulated marked image is to again impart the watermark onto
21 a copy of the unmarked original digitized image, and to use the
22 color planes of that reconstituted marked image as ideal
23 substitutes for the watermarking plane. The disadvantage of this
24 alternative method is that it requires access to a copy of the
25 unmarked original image. The visualizer can also have multiple
26 color planes. The visualizer can be employed without the selector
27 by having at least one statistical value associated with each
28 pixel of the visualizer. Also, sequential repositioning of the
29 selector on the reconstituted watermarking plane need not be
30 non-overlapping. Non-overlapping selector positions in the

1 presented embodiment represent only a computational
2 simplification. Also, a small random but coherent image may be
3 included in the watermarking plane at positions known only to the
4 marker and/or marking entity; if the so constituted watermarking
5 plane were imparted onto a uniform color plane with strong
6 modulation strength, the coherent image would be visible without
7 use of a visualizer. Other methods of watermark detection and/or
8 demonstration may be employed. These may for instance utilize any
9 of the many statistical relationships between elements and their
10 neighbors or non-neighbors. The robust techniques presented here
11 may be used in combination with visible watermarking techniques
12 as well as fragile invisible techniques. It will be clear to
13 those skilled in the art that other modifications to the
14 disclosed embodiments can be effected without departing from the
15 spirit and scope of the invention.

16 The present invention can also be realized in embodiments of an
17 apparatus having mechanisms for implementing the methods of the
18 present invention as described herein in manners known to those
19 skilled in the art. For example, the present invention can also
20 be realized as an apparatus to impart a watermark onto a
21 digitized image, said apparatus comprising: means for providing a
22 digitized image having at least one image plane, said image plane
23 being represented by an image array having a plurality of pixels,
24 said pixel having at least one color component, said watermark
25 being formed using a distinct watermarking plane represented by
26 an array having a plurality of distinct watermarking elements,
27 each of said distinct watermarking elements having an array
28 position and having one-to-one positional correspondence with
29 said image pixels; and means for multiplying said brightness data
30 associated with said at least one color component by a

1 predetermined brightness multiplying factor, wherein said
2 brightness multiplying factor is a corresponding distinct
3 watermarking element, said distinct watermarking element being in
4 the domain of 0.5 to 1.0. Thus in an embodiment the present
5 invention can also be realized as an apparatus for imparting a
6 watermark onto a digitized image comprising the steps of: means
7 for providing said digitized image comprised of a plurality of
8 pixels, wherein each of said pixels includes brightness data that
9 represents a brightness of at least one color; and means for
10 multiplying said brightness data associated with at least one of
11 said pixels by a predetermined brightness multiplying factor in
12 the domain of 0.5 to 1.0. In a particular embodiment of the
13 apparatus the image has I rows and J columns, and has a pixel in
14 row i and column j having a brightness $Y(i,j)$, and the means for
15 multiplying includes: means for adding to or subtracting from the
16 brightness $Y(i,j)$ a different small random value $\epsilon(i,j)$, wherein
17 $1 \leq i \leq I$ and $1 \leq j \leq J$ are the row and column indices of a pixel
18 location in the image.

19 Thus in an embodiment the present invention can also be realized
20 as an apparatus for imparting a watermark onto a digitized image
21 comprising: means for providing said digitized image comprised of
22 a plurality of pixels, wherein each of said pixels includes
23 brightness data that represents a brightness of at least one
24 color, with said image having I rows and J columns, and a pixel
25 in row i and column j having a brightness $Y(i,j)$; and means for
26 adding to or subtracting from the brightness $Y(i,j)$, for all i
27 and all j, a random value $\epsilon(i,j)$, wherein $1 \leq i \leq I$ and $1 \leq j \leq J$
28 are the row and column indices of a pixel location in the image.

1 Thus in an embodiment the present invention can also be realized
2 as an apparatus for generating a watermarked image, the apparatus
3 comprising: means for imparting a watermark onto a digitized
4 image having a plurality of original pixels, each of said pixels
5 having original brightness values; means for providing said
6 digitized watermarking plane comprising a plurality of
7 watermarking elements, each element having a watermark brightness
8 multiplying factor and having one-to-one positional
9 correspondence with said original pixels; and means for producing
10 a watermarked image by multiplying said original brightness
11 values of each of said original pixels by said brightness
12 multiplying factor of a corresponding one of said watermark
13 elements.

14 Thus in an embodiment the present invention can also be realized
15 as an apparatus comprising: means for forming a watermarking
16 plane including a plurality of elements each having a brightness
17 adding or subtracting value; means for generating a robust random
18 sequence of integers having a first plurality of bits; means for
19 linearly remapping said random sequence to form a remapped
20 sequence of brightness multiplying factors to provide a desired
21 modulation strength; means for computing a discrete Fourier
22 transform of said remapped sequence to form a Fourier sequence
23 having frequency coordinates; means for expanding said frequency
24 coordinates to form an expanded sequence; means for computing an
25 inverse Fourier transform of said expanded sequence to obtain a
26 watermarking sequence of values; and means for deriving said
27 brightness adding or subtracting values of said elements of said
28 watermarking plane based upon said watermarking sequence of
29 values.

1 Thus in an embodiment the present invention can also be realized
2 as an apparatus for detecting a watermarking plane comprising:
3 means for providing an image having a plurality of pixels marked
4 by the watermarking plane, said watermarking plane having a
5 plurality of watermarking elements; means for aligning said
6 watermarking plane with said image; means for identifying a
7 subset of said image pixels; means for each image pixel, $u(i,j)$,
8 wherein $1 \leq i \leq I$ and $1 \leq j \leq J$, of said subset of image pixels,
9 including means for generating a first value representing a
10 relationship between an attribute of said image pixel $u(i,j)$ and
11 an attribute of image pixels that neighbor said image pixel
12 $u(i,j)$; means for identifying a watermarking element $w(i,j)$ that
13 positionally corresponds to said image pixel $u(i,j)$ and
14 watermarking elements that correspond to said image pixels that
15 neighbor said image pixel $u(i,j)$; means for generating a second
16 value representing a relationship between an attribute of said
17 watermarking element $w(i,j)$ and an attribute of the identified
18 neighboring watermarking elements; and means for generating a
19 coincidence value representing likelihood that said image is
20 marked by said watermarking plane based upon said first and
21 second values.

22 Thus in an embodiment the present invention can also be realized
23 as an apparatus comprising means for generating a visual
24 representation of a data array of data elements having a data
25 array size, including: means for providing a
26 visualizer-coincidence pattern of visualizer-coincidence image
27 pixels represented by a visualizer-coincidence array of
28 visualizer-coincidence pixels, said visualizer-coincidence array
29 having an array size equal to said data array size, wherein each
30 of said visualizer-coincidence pixels has a first color if a

1 corresponding data element is a first logical value and a second
2 color if said corresponding data element has a complementary
3 logical value; means for setting said visualizer-coincidence
4 pixel to a first color if a value of said data element is above a
5 predetermined threshold and to another color if said value is
6 below said predetermined threshold; and means for displaying said
7 visualizer-coincidence image to form said visual representation.

8 Thus in an embodiment the present invention can also be realized
9 as an apparatus for imparting a watermark onto a digitized image
10 comprising: means for providing said digitized image comprised of
11 a plurality of pixels, wherein each of said pixels includes
12 brightness data represented by at least one color component, Y;
13 and means for adding to or subtracting from said brightness data
14 associated with at least one of said pixels a predetermined
15 brightness adding or subtracting factor in the range of $-0.5Y$ to
16 $+0.5Y$, wherein said brightness adding or subtracting factor has a
17 relationship with a number taken from a random number sequence,
18 said relationship is a linear remapping to provide a desired
19 modulation strength, and said modulation strength is less than 50
20 percent.

21 Thus in an embodiment the present invention can also be realized
22 as an apparatus for imparting a watermark onto a digitized image
23 comprising: means for providing said digitized image comprised of
24 a plurality of pixels, wherein each of said pixels includes
25 brightness data represented by at least one color component, Y;
26 and means for adding to or subtracting from said brightness data
27 associated with at least one of said pixels by a predetermined
28 brightness adding or subtracting factor in the range of $-0.5Y$ to
29 $+0.5Y$, wherein said brightness adding or subtracting factor has a

1 relationship with a number taken from a random number sequence,
2 said relationship is a linear remapping to provide a desired
3 modulation strength, said sequence is formed from a plurality of
4 robust watermarking parameters, and said parameters comprise a
5 cryptographic key, two coefficients and an initial value of said
6 random number generator.

7 The present invention can be realized in hardware, software, or a
8 combination of hardware and software. A visualization tool
9 according to the present invention can be realized in a
10 centralized fashion in one computer system, or in a distributed
11 fashion where different elements are spread across several
12 interconnected computer systems. Any kind of computer system - or
13 other apparatus adapted for carrying out the methods and/or
14 functions described herein - is suitable. A typical combination
15 of hardware and software could be a general purpose computer
16 system with a computer program that, upon being loaded and
17 executed, controls the computer system such that it carries out
18 the methods described herein. The present invention can also be
19 embedded in a computer program product, which comprises all the
20 features enabling the implementation of the methods described
21 herein, and which - when loaded in a computer system - is able to
22 carry out these methods.

23 Computer program means or computer program in the present context
24 include any expression, in any language, code or notation, of a
25 set of instructions intended to cause a system having an
26 information processing capability to perform a particular
27 function either directly or after either or both of the
28 following: conversion to another language, code or notation,
29 and/or reproduction in a different material form.

1 Thus the invention includes an article of manufacture comprising
2 a computer usable medium having computer readable program code
3 means embodied therein for causing a function described above.
4 The computer readable program code means in the article of
5 manufacture comprises computer readable program code means for
6 causing a computer to effect the steps of a method of this
7 invention. Similarly, the present invention may be implemented as
8 a computer program product comprising a computer usable medium
9 having computer readable program code means embodied therein for
10 causing a function described above. The computer readable program
11 code means in the computer program product comprises computer
12 readable program code means for causing a computer to effect one
13 or more functions of this invention. Furthermore, the present
14 invention may be implemented as a program storage device readable
15 by machine, tangibly embodying a program of instructions
16 executable by the machine to perform method steps for causing one
17 or more functions of this invention.

18 It is noted that the foregoing has outlined some of the more
19 pertinent objects and embodiments of the present invention. This
20 invention may be used for many applications. Thus, although the
21 description is made for particular arrangements and methods, the
22 intent and concept of the invention is suitable and applicable to
23 other arrangements and applications. It will be clear to those
24 skilled in the art that modifications to the disclosed
25 embodiments can be effected without departing from the spirit and
26 scope of the invention. The described embodiments ought to be
27 construed to be merely illustrative of some of the more prominent
28 features and applications of the invention. Other beneficial
29 results can be realized by applying the disclosed invention in a

- 1 different manner or modifying the invention in ways known to
- 2 those familiar with the art.

00931210-081501
TOSTED-012TE660